AMENDED EXHIBIT H

Amended Claim Chart for U.S. Patent No. 9,665,705 (“the ’705 Patent”)

The Accused Instrumentalities include Apple devices with Touch ID or Face ID, including iPhone, iPad, Mac, and any Apple product or device that is substantially or reasonably similar to the functionality set forth below. The Accused Instrumentalities infringe the claims of the ’705 Patent, as described below, either directly under 35 U.S.C. § 271(a), or indirectly under 35 U.S.C. §§ 271(b)–(c). The Accused Instrumentalities infringe the claims of the ’705 Patent literally and, to the extent not literally, under the doctrine of equivalents.

Claim 1	**Accused Instrumentalities**
1. A system for providing secure access to a controlled item, the system comprising:	***To the extent that the preamble is deemed to be a limitation, the Accused Instrumentalities are configured to use a system in accordance with this claim.*** As further explained below, the Accused Instrumentalities consist of an Apple device with a biometric unlock function, including Touch ID and Face ID. The biometric unlock function is incorporated in the Accused Instrumentalities providing for secure access to the Accused Instrumentalities. (*See* Ex. A, Apple Platform Security at 7, 9, 24 and 86 (defining Data Protection classes, including Complete Protection (NSFFileProtectionComplete))). The following Apple devices include either a Touch ID or Face ID feature: 1. iPhone (Touch ID or Face ID) 2. iPad (Touch ID or Face ID) 3. MacBook (Touch ID) 4. Mac with Magic Keyboard (Touch ID) These Accused Instrumentalities are the controlled items.
1a. a memory comprising a database of biometric signatures;	***The Accused Instrumentalities include a memory comprising a database of biometric signatures.***

Claim 1	**Accused Instrumentalities**
	Touch ID: The iPhone and iPad allow a user to "[r]egister up to five fingerprints." (https://support.apple.com/en-us/HT201371) On a Mac, users "can add up to three fingerprints to [their] user account." Across all user accounts, the Mac "can save up to five fingerprints." Fingerprints stored on different accounts allow users to quickly switch between those accounts. (https://support.apple.com/guide/mac-help/use-touch-id-mchl16fbf90a/12.0/mac/12.0; https://www.imore.com/how-use-touch-id-your-macbook-pro; https://eshop.macsales.com/blog/75047-set-up-touch-id-on-imac/) **Face ID:** The iPhone and iPad allows the registration of multiple faces. (https://www.macworld.co.uk/how-to/second-face-id-3803421/ (to register a second face, the iPhone offers the option to "set up an alternative appearance"); https://support.apple.com/guide/iphone/set-up-face-id-iph6d162927a/ios ("Set up Face ID or add another face"); https://www.macworld.co.uk/how-to/second-face-id-3803421 ("This second face could belong to a loved one, enabling your partner or child to access your phone without requiring your smiling mug to unlock it")). The Secure Enclave is a system on chip that is included on the Accused Instrumentalities. (Ex. A, Apple Platform Security at 9). "During enrollment, the Secure Enclave processes, encrypts, and stores the corresponding Touch ID and Face ID template data." (*Id.*, at 19). The user's biometric data is stored in a nonvolatile storage device assigned to the Secure Enclave in the Accused Instrumentalities. (*Id.* at 9, 15, and 16).
1b. a transmitter sub-system comprising:	***As set forth in elements 1b1, 1b2, and 1b3 below, the Accused Instrumentalities include a transmitter sub-system.***

Claim 1	**Accused Instrumentalities**
1b1. a biometric sensor configured to receive a biometric signal;	***The Accused Instrumentalities include a biometric sensor configured to receive a biometric signal.*** **Touch ID:** The Accused Instrumentalities equipped with Touch ID have a Touch ID sensor. (Ex. A, Apple Platform Security at 19). "When the fingerprint ***sensor*** detects the touch of a finger, it triggers the advanced imaging array to scan the finger." (*Id.* (emphasis added)) "The Touch ID ***sensor*** [for iPhone and iPad] is located either in the Home button or—on the iPad Air (4th generation)—the top button." (https://support.apple.com/en-us/HT201371 (emphasis added)) On Mac computers, including Mac notebook computers and iMacs paired with the Magic Keyboard, "[t]he Touch ID ***sensor*** is located in the upper-right corner of your keyboard." (https://support.apple.com/en-us/HT212225 (emphasis added); *see also* https://support.apple.com/guide/mac-help/use-touch-id-mchl16fbf90a/12.0/mac/12.0) **Face ID:** The Accused Instrumentalities equipped with Face ID have the TrueDepth camera system, which maps the geometry of a user's face. (Ex. A, Apple Platform Security at 20). "After the TrueDepth camera confirms the presence of an attentive face, it projects and reads over 30,000 infrared dots to form a depth map of the face along with a 2D infrared image." (*Id.*)
1b2. a transmitter sub-system controller configured to match the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute; and	***The Accused Instrumentalities include a transmitter controller configured to match the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute.*** *The Court has construed "accessibility attribute" to mean: "attribute that establishes whether and under which conditions access to the controlled item should be granted to a user."*

Claim 1	**Accused Instrumentalities**
	The Accused Instrumentalities are equipped with a Secure Enclave having a Secure Enclave Processor ("SEP"), which provides the computing power for the Secure Enclave. (Ex. A, Apple Platform Security at 7, 10 and 19). Matching of fingerprint (Touch ID) or facial (Face ID) data is done by the SBIO app on the SEP. (Ex. B, Behind the Scenes With iOS Security at 34; *see also* https://www.youtube.com/watch?v= BLGFriOKz6U (18:07-18:33)). "During matching, the Secure Enclave compares incoming data from the biometric sensor against the stored templates to determine whether to unlock the device or respond that a match is valid (for Apple Pay, in-app, and other uses of Touch ID and Face ID)." (*Id.* at 19). A match of biometric data by the SEP generates a signal providing varying degrees of access to the subject Accused Instrumentality. (Ex. A, Apple Platform Security at 25). In driving mode, i.e., when an iPhone's sensors detect motion and driving mode is turned on, a user whose biometric data matches the data stored in the iPhone database (discussed below), will be granted access to iPhone functionality if the user also taps "I'm Not Driving." (https://www.alphr.com/disable-are-you-driving-iphone/). In the event that the Use Screen Time Passcode is set, a user whose biometric data matches the data stored in the iPhone database (discussed below) will be able to access all data on the iPhone if the user also enters the correct Screen Time passcode. (https://support.apple.com/en-us/HT201304). Otherwise, the user will be unable to access blocked or limited apps. (*Id.*) A match of biometric data using Face ID further requires that a user's eyes are open and looking at the screen unless the Require Attention feature is turned off. (https://support.apple.com/guide/iphone/face-id-attention-iph646624222/ios).

Claim 1	**Accused Instrumentalities**
	In the event that a user's biometric data does not match the data stored in the iPhone database (discussed below), the user is nonetheless allowed to access the iPhone to make an emergency call, in which case the iPhone also sends out an alert to the emergency contacts stored in the iPhone. (https://support.apple.com/en-us/HT208076). On Mac computers, once an authorized user logs into an account, that user can quickly re-log into that account (e.g., after the computer has gone to sleep) and access additional features (e.g., make payments via Apple Pay or log into an account or website) via the Touch ID sensor. The ability to use biometric recognition is also conditioned on the fact that a fingerprint has not been rejected five times in a row and the device has not been locked for more than 48 continuous hours. (https://support.apple.com/en-us/HT212225) "When two or more users are logged in [to a Mac computer] at the same time, you can quickly switch between users using Touch ID." The user can be switched so long as the following conditions are met: the received fingerprint matches a stored fingerprint for a user with a different account and an administrator has enabled the "fast user switching" feature in the System Preferences app. (https://support.apple.com/guide/mac-help/switch-quickly-between-users-mchlp2439/mac) One such use of fast switching is to switch between an administrator account and a non-administrator or ordinary account. While logged into the ordinary account, an administrator can place a finger on the Touch ID sensor and switch to the administrator account (e.g., to change settings which require administrator privileges). Similarly, an ordinary user can switch to their account via a press of the Touch ID sensor. (*Id.*) The conditions under which access allowed to an Accused Instrumentality in the event of a biometric data match is controlled by various parameters associated with such matching. [redacted] (APL-CPC_SC_000054-55), lines 322-361. For example, in the file [redacted], the term [redacted]. (APL-CPC_SC_000054, line 337) [redacted]

Claim 1	**Accused Instrumentalities**
	i [redacted] (*Id.*) [redacted] (APL-CPC_SC_000057–58 ([redacted]) and APL-CPC_SC_000058 [redacted]).
1b3. a transmitter configured to emit a secure access signal conveying information dependent upon said accessibility attribute; and	***The Accused Instrumentalities include a transmitter configured to emit a secure access signal conveying information dependent upon said accessibility attribute.*** If access to an Accused Instrumentality is to be granted, the Secure Enclave re-encrypts (re-wraps) a file key with an ephemeral key (which is only generated if access is to be granted), and sends the re-encrypted file key to the file system driver of the application processor. (Ex. A, Apple Platform Security at 14, 24 and 85; Ex. B, Behind the Scenes with iOS Security, at 29–30; *see also* https://www.youtube.com/watch?v= BLGFriOKz6U (12:13-12:51)). On a successful match, the Secure Enclave acts as a transmitter in order to emit the re-wrapped file key to the application processor for unwrapping the Data Protection keys, unlocking the device or account. (Ex. A, Apple Platform Security at 14, 24 and 85).
1c. a receiver sub-system comprising:	***As set forth in elements 1c1 and 1c2 below, the Accused Instrumentalities include a receiver sub-system.***
1c1. a receiver sub-system controller configured to: receive the transmitted secure access signal; and	***The Accused Instrumentalities include a receiver sub-system controller configured to: receive the transmitted secure access signal.*** The re-wrapped file key transmitted by the Secure Enclave is received by the file system driver of the application processor, which acts as the receiver sub-system controller. Specifically, the receiver is the "dedicated AES256 crypto engine (the "AES Engine") built into the direct memory access

Claim 1	**Accused Instrumentalities**
	path…." "The Secure Enclave [transmitter sub-system controller] transmits this key to the AES Engine [receiver sub-system controller] using dedicated wires…." (Ex. A, Apple Platform Security at 14 and 85).
1c2. provide conditional access to the controlled item dependent upon said information;	***The Accused Instrumentalities include a receiver sub-system configured to provide conditional access to the controlled item dependent upon said information.*** Once the re-wrapped file key is received by the system driver of the application processor, it is provided to the AES Engine, which decrypts it the file key, whereupon the AES Engine has access to the encrypted files, providing access thereto to the user. (Ex. A, Apple Platform Security at 7, 14 and 85).
1d. wherein the transmitter sub-system controller is further configured to:	***The Accused Instrumentalities include a transmitter sub-system controller that is configured to be used as set forth in elements 1d1, 1d2, and 1d3 below.***
1d1. receive a series of entries of the biometric signal, said series being characterized according to at least one of the number of said entries and a duration of each said entry;	***The Accused Instrumentalities include a transmitter sub-system controller configured to receive a series of entries of the biometric signal, said series being characterized according to at least one of the number of said entries and a duration of each said entry.*** *The Court has construed "at least one of the number of said entries and a duration of each said entry" to mean: "'at least' modifies 'one of the number of said entries.' The claim additionally requires 'a duration of each said entry.'"* **Touch ID:** A user's fingerprint is registered "by raising and slowly lowering" the user's finger over and over again (a "number" of times), "changing the position of [the] finger just a tiny bit at a time."

Claim 1	**Accused Instrumentalities**
	(https://support.apple.com/en-us/HT201371; https://www.youtube.com/watch?v=xTZ2LALWZlg&ab_channel=AppleSupport) The user's finger must remain on the home button long enough for the data to be recorded (a minimum "duration"). Apple directs users to "[t]ouch the Touch ID sensor with your finger, but don't press it. Hold it there [for a sufficient duration] until you feel a quick vibration, or until you're asked to lift your finger." (https://support.apple.com/en-us/HT201371) The user cannot "tap too quickly" during this registration process," *i.e.,* there is a minimum duration. (https://support.apple.com/en-us/HT207537; *see also* APL-CPC_SC_000076, line 185; APL-CPC_SC_000113, line 54 [redacted]; *see also* (APL-CPC_SC_000101, line 35) [redacted]. **Face ID:** The TrueDepth camera of the iPhone "projects and reads over 30,000 infrared dots to form a depth map of the face along with a 2D infrared image." (Ex. A, Apple Platform Security at 20). The user moves his face in front of the camera, which continuously captures the 2D images and depth information. (https://support.apple. com/en-us/HT208109). The user is instructed to "slowly move your head until the circle shown is completed" and "again [for a second time] slowly describe a circle with your head until it is completed" ("number" and "duration"). (https://support.apple.com/en-us/HT208109).
1d2. map said series into an instruction; and	***The Accused Instrumentalities include a transmitter sub-system controller configured to map said series into an instruction.*** **Touch ID:** "The analysis uses subdermal ridge flow angle mapping, a lossy process that discards 'finger minutiae data' that would be required to reconstruct the user's actual fingerprint." (Ex. A,

Claim 1	**Accused Instrumentalities**
	Apple Platform Security at 19). "The sensor captures the biometric image and securely transmits it to the Secure Enclave." (*Id.* at 19). **Face ID:** A mathematical representation of a user's face is calculated during enrollment and transmitted to the Secure Enclave. (*Id.* at 20 and 23).
1d3. populate the database according to the instruction,	***The Accused Instrumentalities include a transmitter sub-system controller configured to populate the database according to the instruction.*** "During enrollment, the Secure Enclave processes, encrypts, and stores the corresponding Touch ID and Face ID template data." (Ex. A, Apple Platform Security at 19). The template data is stored in the secure nonvolatile storage associated with the Secure Enclave. (*Id.*)
1e. wherein the controlled item is one of: a locking mechanism of a physical access structure or an electronic lock on an electronic computing device.	***The Accused Instrumentalities are configured to provide access to the controlled item, wherein the controlled item is one of: a locking mechanism of a physical access structure or an electronic lock on an electronic computing device.*** The controlled items to which access is granted per the above are computing devices. (*See, e.g.,* https://www.britannica.com/technology/iPhone ("iPhone, a multipurpose handheld computing device . . .")). Apple iPad and Mac computers are also computing devices.

Claim 10	**Accused Instrumentalities**
10. A transmitter sub-system for operating in a system for providing secure access to a controlled item, wherein the transmitter sub-system comprises:	***To the extent that the preamble is deemed to be a limitation, the Accused Instrumentalities are configured to use a system in accordance with this claim.***
10a. a biometric sensor configured to receiving a biometric signal;	***The Accused Instrumentalities include a biometric sensor configured to receive a biometric signal.*** See Claim 1b1 above.
10b. a controller configured to match the biometric signal against members of a database of biometric signatures to thereby output an accessibility attribute; and	***The Accused Instrumentalities include a controller configured to match the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute.*** See Claim 1b2 above.
10c. a transmitter configured to emit a secure access signal conveying said information dependent upon said accessibility attribute;	***The Accused Instrumentalities include a transmitter configured to emit a secure access signal conveying information dependent upon said accessibility attribute.*** See Claim 1b3 above.
10d. wherein the controller is further configured to:	***The Accused Instrumentalities include a controller that is configured to be used as set forth in elements 10d1, 10d2, and 10d3 below.***

Claim 10	**Accused Instrumentalities**
10d1. receive a series of entries of the biometric signal, said series being characterised according to at least one of the number of said entries and a duration of each said entry;	***The Accused Instrumentalities include a transmitter sub-system controller configured to receive a series of entries of the biometric signal, said series being characterized according to at least one of the number of said entries and a duration of each said entry.*** See Claim 1d1 above.
10d2. map said series into an instruction; and	***The Accused Instrumentalities include a transmitter sub-system controller configured to map said series into an instruction.*** See Claim 1d2 above.
10d3. populate the database according to the instruction, wherein the controlled item is one of: a locking mechanism of a physical access structure or an electronic lock on an electronic computing device.	***The Accused Instrumentalities include a controller configured to populate the database according to the instruction, wherein the controlled item is one of: a locking mechanism of a physical access structure or an electronic lock on an electronic computing device.*** See Claim 1d3 and Claim 1e above. Claim 1d3 describes how the controller populates a database according to the instruction, and Claim 1e describes how the controlled item is one of a locking mechanism of a physical access structure or an electronic lock on an electronic computing device.

Claim 11	**Accused Instrumentalities**
11. A method for providing secure access to a controlled item in a system comprising a database of biometric signatures, a transmitter sub-system comprising a biometric sensor configured to receive a biometric signal, and a transmitter configured to emit a secure access signal capable of granting access to the controlled item, and a receiver sub-system comprising a receiver sub-system controller configured to receive the transmitted secure access signal, and provide conditional access to the controlled item dependent upon information in said secure access signal, the method comprising:	***To the extent that the preamble is deemed to be a limitation, the Accused Instrumentalities are configured to use a method in accordance with this claim.*** *See* Claim 1.
11a. populating the database of biometric signatures by:	***The Accused Instrumentalities are configured to populate the database of biometric signatures as set forth in elements 11a1, 11a2, and 11a3 below.***

Claim 11	**Accused Instrumentalities**
11a1. receiving a series of entries of the biometric signal;	***The Accused Instrumentalities are configured to populate the database of biometric signatures by: receiving a series of entries of the biometric signal.*** See Claim 1d1 above.
11a2. determining at least one of the number of said entries and a duration of each said entry;	***The Accused instrumentalities are configured to populate the database of biometric signatures by: determining at least one of the number of said entries and a duration of each said entry.*** See Claim 1d1 above.
11a3. mapping said series into an instruction; and	***The Accused instrumentalities is configured to populate the database of biometric signatures by: mapping said series into an instruction.*** See Claim 1d2 above.
11a4. populating the database according to the instruction;	***The Accused instrumentalities are configured to populate the database according to the instruction.*** See Claim 1d3 above.
11b. receiving the biometric signal;	***The Accused Instrumentalities include a biometric sensor configured to receive the biometric signal.*** See Claim 1b1 above.

Claim 11	**Accused Instrumentalities**
11c. matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute;	***The Accused Instrumentalities are configured to match the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute.*** See Claim 1b2 above.
11d. emitting a secure access signal conveying information dependent upon said accessibility attribute; and	***The Accused Instrumentalities are configured to emit a secure access signal conveying information dependent upon said accessibility attribute.*** See Claim 1b3 above.
11e. providing conditional access to the controlled item dependent upon said information, wherein the controlled item is one of: a locking mechanism of a physical access structure or an electronic lock on an electronic computing device.	***The Accused Instrumentalities are configured to provide conditional access to the controlled item dependent upon said information, wherein the controlled item is one of: a locking mechanism of a physical access structure or an electronic lock on an electronic computing device.*** See Claim 1c2 and Claim 1e above. Claim 1c2 describes the step of providing conditional access to the controlled information, and Claim 1e describes how the controlled item is one of a locking mechanism of a physical access structure or an electronic lock on an electronic computing device.

Claim 15	**Accused Instrumentalities**
15. A system for providing secure access to a controlled item, the system comprising:	***The Accused Instrumentalities are non-transitory computer readable storage medium storing a computer program comprising instructions as set forth below.***
15a. a memory comprising a database of biometric signatures;	***The Accused Instrumentalities include a memory comprising a database of biometric signatures.*** See Claim 1a above.
15b. a transmitter sub-system comprising:	***As set forth in elements 15b1, 15b2, and 15b3 below, the Accused Instrumentalities include a transmitter subsystem*** See Claim 1b above.
15b1. a biometric sensor capable of receiving a biometric signal;	***The Accused Instrumentalities include a biometric sensor configured to receive a biometric signal.*** See Claim 1b1 above.
15b2. a transmitter sub-system controller capable of matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute; and	***The Accused Instrumentalities include a transmitter sub-system controller capable of matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute.*** See Claim 1b2 above.

Claim 15	**Accused Instrumentalities**
15b3. a transmitter capable of emitting a secure access signal conveying information dependent upon said accessibility attribute; and	***The Accused Instrumentalities include a transmitter capable of emitting a secure access signal conveying information dependent upon said accessibility attribute.*** See Claim 1b3 above.
15c. a receiver sub-system comprising:	***As set forth in elements 15c1 and 15c2 below, the Accused Instrumentalities include a receiver sub-system.*** See Claim 1c above.
15c1. a receiver sub-system controller capable of: receiving the transmitted secure access signal; and	***The Accused Instrumentalities include a receiver sub-system controller capable of: receiving the transmitted secure access signal.*** See Claim 1c1 above.
15c2. providing conditional access to the controlled item dependent upon said information;	***The Accused Instrumentalities include a receiver sub-system configured to provide conditional access to the controlled item dependent upon said information.*** See Claim 1c2 above.
15d. wherein the transmitter sub-system controller is further capable of:	***The Accused Instrumentalities include a transmitter sub-system controller that is configured to be used as set forth in elements 15d1, 15d2, and 15d3 below.*** See Claim 1d above.

Claim 15	**Accused Instrumentalities**
15d1. receiving a series of entries of the biometric signal, said series being characterised according to at least one of the number of said entries and a duration of each said entry;	***The Accused Instrumentalities include a transmitter sub-system controller configured to receive a series of entries of the biometric signal, said series being characterized according to at least one of the number of said entries and a duration of each said entry.*** See Claim 1d1 above.
15d2. mapping said series into an instruction; and	***The Accused Instrumentalities include a transmitter sub-system controller configured to map said series into an instruction.*** See Claim 1d2 above.
15d3. populating the data base according to the instruction,	***The Accused Instrumentalities include a transmitter sub-system controller configured to populate the database according to the instruction.*** See Claim 1d3 above.
15e. wherein the controlled item is one of: a locking mechanism of a physical access structure or an electronic lock on an electronic computing device.	***The Accused Instrumentalities are configured to provide access to the controlled item, wherein the controlled item is one of: a locking mechanism of a physical access structure or an electronic lock on an electronic computing device.*** See Claim 1e above.

Claim 16	**Accused Instrumentalities**
16. A transmitter sub-system for operating in a system for providing secure access to a controlled item, wherein the transmitter sub-system comprises:	***To the extent that the preamble is deemed to be a limitation, the Accused Instrumentalities include a transmitter sub-system for operating in a system for providing secure access to a controlled item in accordance with this claim.***
16a. a biometric sensor capable of receiving a biometric signal;	***The Accused Instrumentalities include a biometric sensor capable of receiving a biometric signal.*** See Claim 1b1 above.
16b. a controller capable of matching the biometric signal against members of a database of biometric signatures to thereby output an accessibility attribute; and	***The Accused Instrumentalities include a controller capable of matching the biometric signal against members of a database of biometric signatures to thereby output an accessibility attribute.*** See Claim 1b2 above.
16c. a transmitter capable of emitting a secure access signal conveying said information dependent upon said accessibility attribute;	***The Accused Instrumentalities include a transmitter capable of emitting a secure access signal conveying said information dependent upon said accessibility attribute.*** See Claim 1b3 above.
16d. wherein the controller is further capable of:	***The Accused Instrumentalities include a controller that has capabilities as set forth in elements 16d1, 16d2, and 16d3 below.***

<u>**Claim 16**</u>	<u>**Accused Instrumentalities**</u>
16d1. receiving a series of entries of the biometric signal, said series being characterised according to at least one of the number of said entries and a duration of each said entry;	***The Accused Instrumentalities include a transmitter sub-system controller configured to receive a series of entries of the biometric signal, said series being characterized according to at least one of the number of said entries and a duration of each said entry.*** See Claim 1d1 above.
16d2. mapping said series into an instruction; and	***The Accused Instrumentalities include a controller capable of: mapping said series into an instruction.*** See Claim 1d2 above.
16d3. populating the database according to the instruction,	***The Accused Instrumentalities include a controller capable of: populating the database according to the instruction.*** See Claim 1d3 above.
16e. wherein the controlled item is one of: a locking mechanism of a physical access structure or an electronic lock on an electronic computing device.	***The Accused Instrumentalities include a controller capable of: populating the database according to the instruction, wherein the controlled item is one of: a locking mechanism of a physical access structure or an electronic lock on an electronic computing device.*** See Claim 1e above.

Claim 17	**Accused Instrumentalities**
17. A method for providing secure access to a controlled item in a system comprising a database of biometric signatures, a transmitter sub-system comprising a biometric sensor capable of receiving a biometric signal, and a transmitter capable of emitting a secure access signal capable of granting access to the controlled item, and a receiver sub-system comprising a receiver sub-system controller capable of receiving the transmitted secure access signal, and providing conditional access to the controlled item dependent upon information in said secure access signal, the method comprising:	***To the extent that the preamble is deemed to be a limitation, the Accused Instrumentalities are configured to use a method in accordance with this claim.*** See Claims 1 and 11 above.
17a. populating the database of biometric signatures by:	***The Accused Instrumentalities are configured to populate the database of biometric signatures as set forth in elements 17a1 to 17a4 below.***

Claim 17	**Accused Instrumentalities**
17a1. receiving a series of entries of the biometric signal;	***The Accused Instrumentalities are configured to populate the database of biometric signatures by: receiving a series of entries of the biometric signal.*** See Claim 1d1 above.
17a2. determining at least one of the number of said entries and a duration of each said entry;	***The Accused instrumentalities are configured to populate the database of biometric signatures by: determining at least one of the number of said entries and a duration of each said entry.*** See Claim 11b above.
17a3. mapping said series into an instruction; and	***The Accused Instrumentalities are configured to populate the database of biometric signatures by: mapping said series into an instruction.*** See Claim 1d2 above.
17a4. populating the database according to the instruction;	***The Accused Instrumentalities are configured to populate the database of biometric signatures by: populating the database according to the instruction.*** See Claim 1d3 above.
17b. receiving the biometric signal;	***The Accused Instrumentalities are configured to receive the biometric signal.*** See Claim 1b1 above.

Claim 17	**Accused Instrumentalities**
17c. matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute;	***The Accused Instrumentalities are configured to match the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute.*** See Claim 1b2 above.
17d. emitting a secure access signal conveying information dependent upon said accessibility attribute; and	***The Accused Instrumentalities are configured to emit a secure access signal conveying information dependent upon said accessibility attribute.*** See Claim 1b3 above.
17e. providing conditional access to the controlled item dependent upon said information, wherein the controlled item is one of: a locking mechanism of a physical access structure or an electronic lock on an electronic computing device.	***The Accused Instrumentalities are configured to provide conditional access to the controlled item dependent upon said information.*** See Claim 1c2 and Claim 1e above. Claim 1c2 describes the step of providing conditional access to the controlled information, and Claim 1e describes how the controlled item is one of a locking mechanism of a physical access structure or an electronic lock on an electronic computing device.